

REMARKS

The Office examined claims 1-3, 5-8, 10-11, and 14-24 and rejected same. With this paper, reconsideration is requested.

Rejections under 35 USC §101

At section 4 of the Office action, claim 15 is rejected under 35 USC §101 as directed to non-statutory subject matter, i.e. to software *per se*.

First, a policy-based argument that claim 15 is statutory: Applicant respectfully points out that the purpose of a claim is to provide notice to the public of subject matter for which there is a right to exclude. Claim 15 is recited as directed to a user equipment terminal. Applicant respectfully submits that the public would not read such a claim as directed to software *per se*. Instead, the public would understand claim 15 to require hardware including memory storage and a processor, and that the recited functionality provided by "an application" and the recited functionality provided by "a business relationship manager" must both be understood as software stored in the memory storage, in a form suitable for execution by the processor.

Second, a more legally cognizable argument that claim 15 is statutory:

The MPEP @ 2111.02 also provides that:

..."If the claim preamble, when read in the context of the entire claim, recites limitations of the claim, or, if the claim preamble is 'necessary to give life, meaning, and vitality' to the claim, then the claim preamble should be construed as if in the balance of the claim." Pitney Bowes, Inc. v. Hewlett-Packard Co., 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999). ... Kropa v. Robie, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951) (A preamble reciting "An abrasive article" was deemed essential to point out the invention defined by claims to an article comprising

abrasive grains and a hardened binder and the process of making it. The court stated "it is only by that phrase that it can be known that the subject matter defined by the claims is comprised as an abrasive article. Every union of substances capable inter alia of use as abrasive grains and a binder is not an 'abrasive article.'" Therefore, the preamble served to further define the structure of the article produced.) [Emphasis added.]

Here, without the preamble here being given patentable weight, the body of the claim might be construed as encompassing non-statutory subject matter. But with the preamble construed as limiting, the subject matter must be understood as statutory, i.e. it "further define the structure" of what is claimed. Therefore, the preamble is here "essential to point out the invention defined by [the] claims," and so must be construed as limiting, and therefore the claim encompasses statutory subject matter.

Applicant therefore respectfully submits that claim 15, when fairly read, must be understood as encompassing statutory subject matter.

Accordingly, applicant respectfully requests that the rejection under 35 USC §101 be withdrawn.

Rejections under 35 USC §103

At section 6 of the Office action, claims 1-10, 14-16 and 18 are rejected under 35 USC §103 as being unpatentable over U.S. Pat. Pub. No. 2002/0029347 (hereinafter Edelman), in view of US Pub. No. 2001/0056375 (hereinafter Kunii), and further in view of US Pub. No. 2002/0016748 (hereinafter Emondi). Applicant notes that only claims 1-3, 5-8, 10-11, and 14-24 are now pending, and so applicant understands the rejection at section 6 to be a rejection of only claims 1-3, 5-8, 10, 14-16 and 18.

Of the claims so rejected, claims 1 and 14-16 are each

independent, and the other so rejected claims depend from one or another of claims 1 and 14-16.

As per claims 1 and 14-16: Claim 1 recites a method for use by a business relationship manager hosted by a wireless terminal subscribed to an operator network. The method includes: the business relationship manager receiving from an application hosted by the wireless terminal a request to determine whether the application is registered with the operator network; the business relationship manager then referring to one or more data stores hosting information on registration of applications to determine whether the application is registered with the operator network; and the business relationship manager then signaling to the application that the application is registered if by referring to the one or more data stores the business relationship manager finds that the application is registered, but otherwise displaying options for paying for use of the application, and then in response to an election by a user, registering the application by signaling to the operator network an indication of an elected option for paying for use of the application along with an identifier of the application and a user identifier stored in a subscriber identity module.

Claims 14-16 recite corresponding limitations.

Thus, claims 1 and 14-16 implicitly define "registration" as a process in which an application identifier and an option for paying for use of the application are stored in one or more data stores of an operator network, along with a user identifier.

Edelman discloses a system for protecting against unauthorized access to electronic data stored on an electronic device, i.e. a system that prevents use of electronic data for which there is no proof of a valid "code sequence." Edelman discloses a client program (which may be separate from or

embedded in an application), a licensing medium stored on a smart card in a smart card reader attached to the electronic device, and a registration authority, separate from both the client and licensing medium. Edelman discloses at para. 107, referring to Fig. 7:

[0107] To use the registered software, the user must insert a smart card containing valid license information into the smart card reader of the client computer, i.e., a smart card that has been prepared as described above. As shown in FIG. 7, when the user attempts to activate the software, the client computer checks to see whether a smart card is inserted. If not, the user is prompted to insert the smart card.

[0108] The client program reads the contents of the smart card and verifies that it has not been tampered with. The client program then retrieves the licensing information for the particular software. The licensing information allows the client program to determine whether the user is authorized to use the software and that the authorized period of use or trial use has not expired.

[0109] The client program may use the encrypted hash to detect whether the smart card has been altered. ... This procedure allows the client program to verify the validity of the smart card without communicating with the registration authority.

[0110] Once the verification has been completed, the client program allows the software to be used. ...

"Licensing information" is nowhere explicitly defined, but is indicated at para. 108 as being "information [that] allows the client program to determine whether the user is authorized to use the software and that the authorized period of use or trial use has not expired." At para. 13, in the background section, "registered" software is indicated as software for which a "valid" code sequence can be provided:

The registration program requires the user to enter a code sequence that was provided by the vendor with the software, e.g., printed on a CD-ROM case. The code sequence is checked by the registration program to determine whether it is valid. If it is valid, the registration program enables the user to use the software.

It appears that "licensing information," as used in Edelman, encompasses a code sequence, and possibly other information.

The registration of software per Edelman is explained at paras. 75-82:

[0075] Once the client program has been installed, the installation and registration of protected software proceeds as shown in FIG. 6. The protected software is installed on the client computer, and the user is prompted to register the installed software with the registration authority.

[0076] To register the software, the user must insert a smart card into a reader connected to the computer and must have an Internet connection or modem. ...

[0077] The client program reads the data from the smart card and transmits it to the registration authority along with a set of registration information. The registration authority first compares the smart card data to corresponding data stored in a database to verify that the smart card is valid. The registration authority then compares the registration information to corresponding data stored in a database to verify that the new software registration is authorized.

[0078] The smart card data sent to the registration authority includes a message digest that was generated by a performing a hash function on the smart card data. ... The registration authority compares the message digest to a corresponding entry in the database to verify that the smart card is valid.

...

[0080] The registration information sent to the registration authority includes the unique identifier of the software to be registered. The identifier may be composed of a serial number and a password or passphrase to prevent an unauthorized user from guessing serial numbers. ... The registration authority compares the identifier received with the registration information to a database of valid identifiers provided by the software vendor.

[0081] The registration information sent to the registration authority also includes other information, such as a product number for the software to be registered, a unique smart card serial number, a smart card sequence number. The registration information also includes expiration periods for the smart card and the software licenses, as further discussed below.

[0082] If the registration information is verified by the registration authority, then a new registration entry is created for the newly granted or updated license for the software. The registration authority generates new smart card data reflecting these changes and sends the new data back to the client computer to be stored on the smart card.

So Edelman appears to disclose that to guard against unauthorized use of an application, a client, which may be embedded in the application, is activated when the user attempts to use the application, and then somehow checks that the application is registered by obtaining licensing information from the licensing medium (on the smart card). There is no teaching of how the check is done, nor any teaching of how the client knows how to find the licensing information for the subject application, from among all the applications for which the licensing medium stores licensing information. Para. 108 merely indicates that the client program uses the licensing information to determine "whether the user is authorized to use the software and that the authorized period of use or trial use has not expired." Para. 60 also fails to explain any further, disclosing only that: "the client program communicates with the licensing medium 120 to verify that the user is authorized to access the electronic data." Para. 65 is similar, disclosing only that: "The smart card 120 contains licensing information that indicates to the client program which software the user is authorized to access." Para. 77 discloses the registration authority comparing "the registration information to corresponding data stored in a database to verify that the new software registration is authorized," but this is in the context of newly registering software (see para. 76), and so is not relevant. So Edelman appears to have a major shortcoming in that there is no mechanism disclosed by which the client is able to locate "licensing information" (and "licensing information" is never expressly defined) for a particular application and user, as required by claims 1 and 14-16. (There is extensive disclosure on having the client check that the licensing information stored in the licensing medium is valid, by comparing it with corresponding information at the registration authority, and by

checking that the smart card has not been tampered with, as in para. 108, reproduced above. But there is no teaching of any basis by which the client can locate in the licensing medium license information for the application and for the user (i.e. for some user identifier), as required by claims 1 and 14-16.¹

In contrast, in the invention as in claims 1 and 14-16, since to register an application for a user the business relationship manager provides to the operator network an application identifier (not a serial number indicating a particular copy of an application, but some indicator of the application itself) and a user identifier (as stored in a SIM), it is at least implicit in the invention as in these claims that to check for registration of an application, the business relationship manager uses the same application identifier and user identifier to look up in the recited one or more data stores an indication of whether the user is registered (i.e. has elected a particular option by which to pay for use of the application).

Thus, applicant respectfully submits that Edelman cannot fairly be said to teach referring to one or more data stores hosting information on registration of applications to determine whether the application is registered with the operator network.

Moreover, there is no teaching by Edelman of the business relationship manager (believed equated to Edelman's client by the Examiner) receiving from an application hosted by the wireless terminal a request to determine whether the application is registered with the operator network. The Examiner cites paras. 59 and 60, but these provide only that there is a client program, which may be embedded in the electronic data/ application, and which communicates

¹ Perhaps the client knows an identifier of the application, either an application identifier in the sense used in claims 1 and 14-16 (i.e. indicating the application, not a unique number/ code indicating a particular copy of the application), or else a serial number (i.e. an identifier that is unique among all copies of the application, although possibly the same number as for a copy of another application). Perhaps further, Edelman assumes that if there is any license information on file for one or another kind of these application identifiers, then it is valid (because of the registration process, and because of checking that the licensing medium has not been

with the licensing medium and registration authority:

[0059] As part of such a protection system, the vendor may require the user to install a client program provided by the software protection administrator. The client program installed on the client computer 100 communicates with a licensing information storage medium 120, referred to as the licensing medium, and the registration authority 110. Alternatively, the client program may be embedded in the electronic data and may be executed in the course of accessing the electronic data, rather than being installed separately by the user. The registration authority 110, in turn, communicates with the vendor 130, which maintains a database of valid licenses issued for the electronic data.

[0060] The licensing medium 120 is a portable component that contains information concerning the software or other licensed electronic data that the user is authorized to access. When a user seeks to access a vended piece of electronic data, the client program communicates with the licensing medium 120 to verify that the user is authorized to access the electronic data.

There is no teaching here of the client receiving from the electronic data/ application a request to check for registration.

Further still, the Office asserts (at page 3, beginning at the end of line 6 of section/ paragraph 7 of the Office action) that Edelman discloses "registering the application by signaling to the operator network an indication of an elected option for paying for use of the application along with an identifier of the application and a user identifier stored in a subscriber identity module," citing para. 59, lines 3-10 and para. 65, lines 1-6.

Para. 59 is reproduced above, and para. 65 is:

0065] Referring again to FIG. 1, the client program accesses the smart card 120 using a smart card reader 140 connected to the client computer 100. The smart card 120 contains licensing information that indicates to the client program which software the user is authorized to access. The licensing information may include other information as well, such as for example timestamps that indicate when the license for each authorized software expires.

tampered with). But this is all mere conjecture.

There is thus no teaching in either para. 59 or 65 of signaling an indication of an elected option for paying for use of an application, nor teaching of signaling an identifier of the application, nor teaching signaling a user identifier (let alone a user identifier stored in a subscriber identity module). In relevant part at the cited locations, Edleman teaches only that: "The client program installed on the client computer 100 communicates with a licensing information storage medium 120, referred to as the licensing medium, and the registration authority 110."

But further still, the Office concedes that Edelman does not explicitly teach "displaying options for paying or use of the application, and then in response to an election by a user, registering the application by signaling to the operator network an indication of an elected option for paying for use of the application along with an identifier of the application and a user identifier stored in a subscriber identity module." For this, the Office relies on Kunii, at para. 50, para. 52 lines 3-13, and para. 53, lines 1-7 and 15-21.

Kunii discloses a system for "efficient advertising" (see Abstract), in which advertisements are selected by a "management server" for display by a "performance practicing terminal" based on client information (user registration information) including musical information indicative of a type or model of performance equipment being used by the performance practicing terminal. So Kunii is not in any way concerned with the problem to which Edelman is directed, i.e. "preventing unauthorized access to electronic data stored on an electronic device" (as set out in the abstract of Edelman). Kunii does though use the term "registration," but in Kunii a user registers "for starting new performance training or continuing current performance training." (See para. 50.) Such registering amounts merely to ordering and paying for a new training session (provided by a computer program

application). There is no teaching in Kunii of a business relationship manager receiving a request from an application to check if a user is registered to use the application, and then only if it is determined that the user is not registered, displaying options for paying or use of the application, and then in response to an election by a user, registering the application by signaling to the operator network an indication of an elected option for paying for use of the application along with an identifier of the application and a user identifier stored in a subscriber identity module. Kunii really just teaches allowing a user to purchase an application (a new practice session or continuation of a current practice session) over a network.

Further, the teaching of Kunii of paying for an application (a new practice session or continuation of a current practice session) would change the principle of operation of Edelman, and so by the MPEP at 2143.03 (VI) the teachings of the references are not sufficient to render the claims *prima facie* obvious. Edleman teaches protecting against unauthorized access to electronic data by checking that the electronic data has been properly registered, i.e. that valid license information is on file (in the licensing medium, and that the licensing medium has not been tampered with). Edelman does not teach buying an application over a network, which is all that is taught by Kunii, in relevant part. The invention is aimed at allowing for use of applications installed on a cell phone (legally, by a manufacturer or cell phone provider), and then paid for only if the user wants to use them. As explained at page 1 of the application:

In case of telecommunications, the development of new applications is critical to the continued evolution of the state of the art. To promote the development of new applications for users of wireless terminals, what is needed is a less cumbersome way to facilitate having a user pay for use of an application hosted by a wireless terminal, ideally

a way that does not involve the user having to transact business with individual application developers, and so a way to pay for an application that is the same regardless of the entity making the application available, and regardless of how the application is installed on the wireless terminal, i.e. regardless of where the application is downloaded from or whether the application is placed in the wireless terminal at the manufacturing facility for the wireless terminal. ...

Edelman, in contrast, is aimed at stopping a user from using illegally copied software. As explained, Edelman discloses a system having as a principle of operation registering properly purchased software (or data) purchased by some means not disclosed by Edelman, and then checking (in a way that is not made clear) for registration of the software any time the user wants to access the software, and denying such access if the check fails. Kunii, in relevant part, is directed to enabling a user to buy a new training session (or continue on with a current training session) over a network. Changing Edelman according to Kunii to arrive at the invention requires changing Edelman to allow for illegal software to be present, and if such is found, to enable the user to pay for it. That's a different principle of operation than Edelman. It would not be problematic to add the teachings of Kunii to those of Edelman so that the purchasing is according to Kunii, followed by registration according to Edelman, followed in turn by checking/ denying access according to Edelman. But to twist Edelman so as to accommodate unregistered and unpaid-for software, and if a user requests access, to provide a means for paying and registering is to engage in hindsight construction, because such a change to Edelman is a change to its principle of operation.

Regarding claim 3, all that is disclosed in paras. 67 and 68 is that registration may be over the Internet. Communication over the Internet may be via http, and so need not be via XML.

Regarding claim 6, the referring to a data store of the

registration authority is disclosed at para. 77 as performed only for (initial) registration. (See para. 76, which sets the context for the disclosure of para. 77.) There is no teaching or disclosure by Edelman of checking with the registration authority each time an attempt is made to access the protected "electronic data."

Regarding claim 8, the Office asserts that Edelman discloses at para. 80, lines 1-3, that "the application is assigned an identifier common to all copies of the application ... and used as an identifier for the application in the one or more data stores" But Edelman discloses there only exactly the opposite!

Para 80 provides:

0080] The registration information sent to the registration authority includes the unique identifier of the software to be registered. The identifier may be composed of a serial number and a password or passphrase to prevent an unauthorized user from guessing serial numbers. The serial number and password are printed on the CD-ROM case in which the software is distributed. Alternatively, the identifier may be generated from two unrelated components, e.g., two words randomly selected from the dictionary. The registration authority compares the identifier received with the registration information to a database of valid identifiers provided by the software vendor.
[Emphasis added.]

A serial number is, by definition, not common to all copies.

Accordingly, for the reasons given and at least by virtue of the dependencies of the claims not argued, applicant respectfully requests that the rejections under 35 USC §103 of claims 1-3, 5-8, 10, 14-16 and 18 be withdrawn.

At section 17 of the Office action, claim 11 is rejected under 35 USC §103 as being unpatentable over Edelman as applied to claim 1, in view of Kunii as applied to claim 1, and further in view of Emondi (also as applied to claim 1) and also further

in view of CGI (Reference U of the PTO-892 attached to the Office action).

Claim 11 depends from claim 1, and is believed allowable over the applied art at least by virtue of its dependency. But further, the Office asserts that the "software accessing the smart card and performing periodic checks" as disclosed in Edleman is the same as the recited application consuming network resources. But the Office has equated "software accessing the smart card and performing periodic checks" to the recited business relationship manager, has equated the "electronic data" of Edleman to the recited "application," and Edelman's "electronic data" is nowhere disclosed as consuming network resources. An example of what is meant by the application consuming network resources is given at page 16, line 13:

For example, the application 11 may be one that provides a weather forecast, and when the user executes the application 11, the application 11 issues a HTTP Get request for information from a network server. The request is passed through the GGSN 15 (Fig. 1) and so there is an opportunity for monitoring the number of such requests (and corresponding replies) made by the application 11, and in fact the invention does make use of the GGSN 15 in providing such an accounting.

Edelman nowhere discloses such an application. Further still, communication with the smart card is not via a network, and so such communication cannot be asserted as consuming network resources. (Note also that the procedure recited in claim 11 by which network resources are requested is directed to enabling charging for the use of network resources as explained at page 16, line 28; but at page 9, line 18, the specification explains that the user is not charged to check for registration, and thus any use of network resources in connection with checking for registration cannot fairly be likened to the application consuming network resources.)

Accordingly, applicant respectfully requests that the rejection under 35 USC §103 of claim 11 be withdrawn.

At section 22 of the Office action, claim 17 is rejected under 35 USC §103 as being unpatentable over Edelman, in view of Kunii, and further in view of Emondi and also CGI.

Claim 17 is believed patentable at least by virtue of its dependency.

Further, the recited "get request" is a request that consumes network resources, and therefore the same arguments used in traversing the rejection of claim 11 are believed to apply also to the rejection of claim 17. In addition, the Office relies on para. 67, lines 8-10, and para. 80, lines 1-3, as teaching "an identifier indicating the application, and communicating the request along with the user and application identifiers to the operator network). But what is recited in claim 17 is a "get request," and all that is discussed by the cited disclosure is a request to register, which is not the same as a "get request" (which results in the network providing the requested data over the network, and so consumes network resources). Edelman nowhere teaches or suggests use of an application for which a get request would be needed. Thus, even though CGI discusses get requests, there is no basis for combining the teachings of CGI with those of Edelman. Even after the combination, there is still no teaching of an application for which a system according to Edelman would provide protection, and which would make a get request.

Accordingly, applicant respectfully requests that the rejection under 35 USC §103 of claim 17 be withdrawn.

At section 23 of the Office action, claims 19 and 22 are rejected under 35 USC §103 as being unpatentable over Kunii, in view of Emondi.

The Office asserts that Kunii discloses "providing to a wireless terminal at least one option for paying for use of an application hosted by the wireless terminal," citing para. 46, lines 10-19 and para. 52, lines 4-15, and "receiving an indication of an option for paying for use of the application along with an identifier of the application," citing para. 53, lines 15-21. Hunii teaches buying over a network "new performance training or new performance training step" (para. 53). Applicant respectfully points out that in both cases, the corresponding application is not hosted by a wireless terminal to be used in the training until the purchase is made. See para. 54, which provides that:

[0054] Namely, upon receipt of the registration information passed from the billing section K3, the training/advertisement setting section K4 generates the program information by reading out, from a program storage section K1 of the server WS, a musical performance training program corresponding to the user-desired training step (i.e. a musical performance training program for a first training step in the case where the "start new performance training" option has been selected by the user, or a musical performance training program for a selected training step in the case where the "continue current performance training" option has been selected by the user. ... The thus-generated program information and advertisement information is transmitted to the performance practicing terminal PC.

Accordingly, applicant respectfully requests that the rejection under 35 USC §103 of claims 19 and 22 be withdrawn.

At section 26 of the Office action, claims 20-21 and 24 are rejected under 35 USC §103 as being unpatentable over Kunii, in view of Emondi and Samjani (Reference V of the PTO-892 attached to the Office action, entitled "General Packet Radio Service (GPRS)."

Claims 20-21 and 24 are believed patentable at least by

virtue of their dependencies. In addition, claim 20 is believed patentable because Kunii does not disclose an application issuing a get request, and although CGI discloses get requests, there is no proper motivation to alter the teaching of Kunii where Kunii teaches a request for a performance training step so as to arrive at the invention, which would require that the software corresponding to the performance training step issue a get request.

Accordingly, applicant respectfully requests that the rejection under 35 USC §103 of claims 20-21 and 24 be withdrawn.

Conclusion


For all the foregoing reasons it is believed that all of the claims of the application are in condition for allowance and their passage to issue is earnestly solicited. Applicant's attorney urges the Examiner to call to discuss the present response if anything in the present response is unclear or unpersuasive.

Respectfully submitted,

June 16, 2007

Date

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468-0224


James A. Retter
Registration No. 41,266

tel: (203) 261-1234
Cust. No.: 004955